

## UNITED STATES DISTRICT COURT

for the  
District of NebraskaIn the Matter of the Search of )  
(Briefly describe the property to be searched or )  
identify the person by name and address) )Information associated with rickpaul38@gmail.com that )  
is stored at premises controlled by Google Inc. )  
1600 Amphitheatre Parkway Mountain View, CA 94043 )

Case No. 8:18MJ324

**SEALED**

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment A.

located in the \_\_\_\_\_ District of \_\_\_\_\_ Nebraska \_\_\_\_\_, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;  
☐ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
21 U.S.C. §841 and 21 U.S.C. §846	Conspiracy to PWID Methamphetamine

The application is based on these facts:

See Attached Affidavit in Support of an Application for a Search Warrant.

- ☒ Continued on the attached sheet.  
☒ Delayed notice of 30 days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

- ☒ Sworn to before me by telephone or other reliable electronic means.

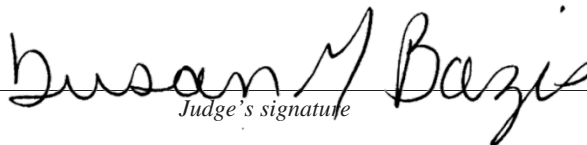
- ☐ Sworn to before me and signed in my presence.

Date: 8-22-18City and state: Omaha, Nebraska

Applicant's signature

SA Frank Feden, US Drug Enforcement Administration

Printed name and title



Judge's signature

SUSAN M. BAZIS U.S. Magistrate Judge

Printed name and title

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEBRASKA**

<b>IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH</b>	)	
	)	<b>Case No. 8:18MJ324</b>
	)	
<u>rickpaul38@gmail.com</u>	)	
	)	
<b>STORED AT</b>	)	<u><b>FILED UNDER SEAL</b></u>
<b>Google, Inc.</b>	)	

**AFFIDAVIT**

I, Frank Feden, being first duly sworn, hereby depose and state as follows:

1. I make this affidavit in support of an application for a search warrant for information associated with the email address rickpaul38@gmail.com, that is stored at premises owned, maintained, controlled, or operated by Google, Inc., an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) to require Google, Inc. to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with rickpaul38@gmail.com, including the contents of communications.
2. I am a Special Agent (SA) with the United States Drug Enforcement Administration (DEA) since May 2003, and I have graduated from the DEA Basic Agent Training in Quantico, Virginia. During my tenure as a Special Agent with the DEA, I have been assigned to investigations of violations of the drug laws of the United States including violations of Title 21, United States Code, Sections 841(a)(1) and Title 21, United States Code, Section 846.
3. In my work as a Special Agent with the DEA, I have been involved in controlled purchases, surveillance, electronic surveillance, arrest of drug traffickers, interviewing of drug traffickers, trash pulls, and the execution of search warrants on residences, businesses, vehicles and electronic devices. As a result, I have arrested individuals for violating State and Federal statutes regarding the possession, manufacture, transportation and sale of controlled substances. I have conducted and have been associated with investigations involving the interception of wire communications and electronic communications obtained from cellular telephone devices and smart phones. I am familiar with the ways in which drug traffickers conduct business, including, but not limited to, their methods of importing and distributing controlled substances, their use of cellular telephones, their use of computers and smart phones and their use of numerical codes and code words to conduct their transactions.
4. I am familiar with the facts and circumstances of this investigation through personal participation and from discussions with agents and officers involved in the investigation. I have also reviewed records and reports related to this investigation. Unless otherwise noted, wherever I assert that a statement was made, the information was provided by another agent, law

enforcement officer or witness, who may have had either direct or hearsay knowledge of that statement, and to whom I, or others, have spoken, or whose reports I have read and reviewed. Such statements are among many statements made by others and are stated in substance and in part unless otherwise indicated. Since this Affidavit is being submitted for the limited purpose of securing search warrant, I have not included details of every aspect of the investigation. Facts not set forth herein, or in the attached exhibits, are not being relied upon in reaching the conclusion that the requested order should be issued. Nor do I request that this Court rely on any facts not set forth herein in reviewing this application.

### **PROBABLE CAUSE**

5. In April 2018, DEA received a tip from Mallinckrodt Pharmaceuticals, a US company, that the company's morphine-sulfate pills were being advertised for sale on the website, [silkroadmeds.com](http://silkroadmeds.com). The representative for Mallinckrodt Pharmaceuticals denied the company had a relationship with [silkroadmeds.com](http://silkroadmeds.com), and the representative claimed that any product purported by [silkroadmeds.com](http://silkroadmeds.com) to be produced by Mallinckrodt Pharmaceuticals was more than likely a counterfeit product.

6. On April 20, 2018, I visited the [silkroadmeds.com](http://silkroadmeds.com) and I observed that numerous brand name pharmaceutical drugs were listed for sale on the site. The site didn't require customers to have a prescription to order controlled substances and it used Western Union and MoneyGram for customers to remit payment.

7. On April 24, 2018, DEA Task Force Officer (TFO) Tyler Kroenke and I accessed the website, "[silkroadmeds.com](http://silkroadmeds.com)", and using an undercover identity, we placed an order for 60 morphine-sulfate 30mg pills and 30 oxycodone 40mg pills. The price for the order was \$456.00 and a prescription was not required to place the order. TFO Kroenke and I, received an email from [sales@silkroadmeds.com](mailto:sales@silkroadmeds.com) directing us to send the payment for the order to Jamshaid MUSHTAQ in Lahore, Pakistan via Money Gram. The email also directed us to send an email to [sales@silkroadmeds.com](mailto:sales@silkroadmeds.com) after the payment had been made.

8. On April 27, 2018, DEA TFO Lee Leighter, acting in an undercover capacity and using DEA buy money, sent the payment to MUSHTAQ via Money Gram. A short time later, I used the undercover computer and the undercover email account to send an email to [sales@silkroadmeds.com](mailto:sales@silkroadmeds.com) indicating the payment had been sent via Money Gram.

9. Money Gram Payment Systems Inc. confirmed that on May 2, 2018, Jamshaid MUSHTAQ presented a Pakistan Government issued identification card to a Money Gram Payment Systems Inc. Agent in Lahore, Pakistan prior to receiving the payment we had sent for the pills.

12. On May 17, 2018, TFO Kroenke checked the undercover email account and discovered the account had received an email from someone claiming to be Baritt LEE using email account [busniesspluss@gmail.com](mailto:busniesspluss@gmail.com). The email indicated that a package had been sent to our shipping address and that the USPS tracking number for that package was RR075512255PH. The email also indicated that the email was sent on behalf of the Silkroad Support Team. TFO Kroenke and I, using the provided tracking number, tracked the package from Manila, Philippines to the undercover United States Post Office Box in Omaha, Nebraska.

13. On June 4, 2018, United States Postal Inspector James Murcek removed the package, which was a small brown paper envelope addressed from Rabab MAMAILAO, Sucat Paranaque Manila, Philippines, 1700 09151692230, from the undercover Post Office Box. Inspector Murcek

then transported the package to the DEA Omaha District Office. TFO Kroenke and I then opened the small brown envelope and discover it contained 50 small round blue pills with "M" imprinted on one side and "30" imprinted on the other side. From my training and experience, I recognized the pills to be Oxycodone 30mg pills manufactured by Mallinckrodt Pharmaceuticals. I then transferred the 50 pills to the DEA North Central Laboratory for analysis.

14. On June 21, 2018, I was notified by a Forensic Chemist from the DEA North Central Laboratory that the 50 pills did not contain Oxycodone. Further, the Chemist explained the pills were made of Heroin, Caffeine, Acetaminophen, Methorphan and 06-Monoacetylmorphine and the pills had been pressed in a pill press to look like Mallinckrodt Pharmaceuticals manufactured Oxycodone 30mg pills.

15. On June 26, 2018, Magistrate Judge Susan M. Bazis of the U.S. District Court, District of Nebraska issued a Search and Seizure Warrant for the email address [businesspluss@gmail.com](mailto:businesspluss@gmail.com). Investigators executed the warrant on June 27, 2018. On June 28, 2018, investigators received the data from Google Inc. with regards to the execution of the Search and Seizure Warrant on for the email address [businesspluss@gmail.com](mailto:businesspluss@gmail.com).

16. The data provided by Google, Inc. for [businesspluss@gmail.com](mailto:businesspluss@gmail.com), listed [rickpaul38@gmail.com](mailto:rickpaul38@gmail.com) as the accounts recovery e-mail. A Gmail recovery email address is an email address that clients of Gmail can list with the company so that if the client becomes locked out of their Gmail account they can have Google, Inc. reset the password and send that new password to them at the recovery e-mail. Google, Inc. also provided phone 923470413699 as the number given to Google by the subscriber as a contact number.

17. The [businesspluss@gmail.com](mailto:businesspluss@gmail.com) contained over 25,000 emails with over 8,000 different email addresses. Almost all of the emails pertained to the sale of controlled and non-controlled prescription drugs, the collection of payment for those drugs and the shipping of those drugs.

18. While searching the e-mails, I found the following automated email which had been sent to [businesspluss@gmail.com](mailto:businesspluss@gmail.com) from [silkroadmeds.com](http://silkroadmeds.com)'s website management software:

A new comment on the post "Ritalin 10mg" is waiting for your approval  
<http://silkroadmeds.com/buy-online/ritalin-methylphenidate-10mg>

**Author: Rick Paul (IP address: 173.244.48.190, ip-190-48-244-173.california.us.northamericancoax.com)**

**Email: [rickpaul38@gmail.com](mailto:rickpaul38@gmail.com)**

**URL:**

**Comment:**

**I had no information about these tablets. Found out about them on the web and I am happy that whatever I had perused was valid. It has worked incredible for me. The delivery is great 13 days for me here in New York.**

19. I also found the following automated email which had been sent to [businesspluss@gmail.com](mailto:businesspluss@gmail.com) from [silkroadmeds.com](http://silkroadmeds.com)'s website management software:

**\_New comment on your post "Xanax (Alprazolam)"**

**Author: Rick Paul (IP address: 173.244.48.190, ip-190-48-244-173.california.us.northamericancoax.com)**

**Email: [rickpaul38@gmail.com](mailto:rickpaul38@gmail.com)**

**URL:**

**Comment:**

**Yet another order. Very fast...10 days, communicates, good quality...5/5 on all categories. Thank you!!**

20. The first email pertains to someone posting a comment on the website in regard to the purchase of Ritalin, which is the brand name for methylphenidate and it is a controlled substance. The second email pertains to someone posting a comment on the website in regard to the purchase of Xanax, which is the brand name for Alprazolam and it is also a controlled substance. The individual posting both comments used rickpaul38@gmail.com to send them. I don't believe the posts were from an actual customer since both emails used the recovery email for businesspluss@gmail.com to send the comments. Additionally, those were the only two emails I found in the 25,000 that were associated with rickpaul38@gmail.com. I did not find any emails associated with rickpaul38@gmail.com involving the purchasing of drugs or receiving of drugs from Silkroadmeds.com. I believe it is more likely that someone involved with silkroadmeds.com made the posts using rickpaul38@gmail.com.

21. On August 10, 2018, I learned from Google, Inc. that the subscriber listed for rickpaul38@gmail.com is Rick Paul. Additionally, Google, Inc. provided phone 923470413699 as the number given to Google by the subscriber as a contact number. That is the same phone number given by the user of businesspluss@gmail.com.

#### **ADDITIONAL INFORMATION**

22. Google, Inc. provides a variety of on-line services, including email access, to the general public. Google, Inc. allows subscribers to obtain email accounts at the domain name gmail.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with Google, Inc. During the registration process, Google, Inc. asks subscribers to provide basic personal information. Therefore, the computers of Google, Inc. are likely to contain stored electronic communications (including retrieved and unretrieved email for Google, Inc. subscribers) and information concerning subscribers and their use of Google, Inc. services, such as account access information, email transaction information, and account application information.

23. In general, an email that is sent to a Google, Inc. subscriber is stored in the subscriber's "mail box" on Google, Inc. computer systems until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google, Inc. computer systems indefinitely. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to Google, Inc.'s computer systems, and then transmitted to its end destination. Google, Inc. often saves a copy of the email sent. Unless the sender of the email specifically deletes the email from the Google, Inc. computer system, the email can remain on the system indefinitely. Even if the sender deletes the e-mail, it may continue to be available on Google's servers for a certain period of time. A sent or received email typically includes the content of the message, source and destination addresses, the date and time at which the email was sent, and the size and length of the email. If an email user writes a draft message but does not send it, that message may also be saved by Google, Inc. but may not include all of these categories of data.

24. A Google, Inc. subscriber can also store files, including emails, address books, contact or buddy lists, calendar data, pictures, and other files, on computer systems maintained and/or owned by Google, Inc.

25. Subscribers to Google, Inc. might not store on their home computers copies of the emails stored in their Google, Inc. account. This is particularly true when they access their Google, Inc. account through the web, or if they do not wish to maintain particular emails or files in their residence.

26. In general, email providers like Google, Inc. ask each of their subscribers to provide certain personal identifying information when registering for an email account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

27. Email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google, Inc.'s website), and other log files that reflect usage of the account. In addition, email providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

28. In some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

29. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

30. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Google, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

31. Based on the provided information, there is probable cause to believe rickpaul38@gmail.com account contains evidence of violations of Title 21, United States Code §§ 841, 846 and other violations of federal code.

32. Based on the forgoing, I request that the court issue the proposed search warrant. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction: as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the court is "a district court of the United States ... that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. 2703(g), the presence of a law enforcement officer is not required for the service or execution of this



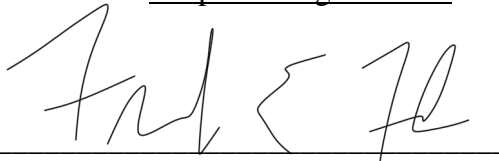
warrant.

**REQUEST FOR SEALING AND ORDER UNDER 18 U.S.C. § 2705**

33. The investigation of the criminal activity discussed above is ongoing and may involve multiple targets, many of whom may not have yet been identified. Moreover, the DEA is not aware of any potential targets that have knowledge of its investigation. Disclosure of the search warrant, this affidavit, or this application may result in the dissemination of these materials to the targets, who may destroy evidence or otherwise evade the investigation. Disclosure of the contents of this affidavit and related documents might have a significant and negative impact on the continuing investigation and might severely jeopardize its effectiveness. Accordingly, I respectfully request that the Court issue an order that the search warrant, this affidavit in support of the application for the search warrant, and the application for the search warrant be filed under seal until further order of this Court. Although the above documents may be sealed, it is respectfully requested that the data obtained as a result of the search warrant may be disclosed to third parties to facilitate analysis. I further request that the Court issue an order commanding Google, Inc, not notify any person of the existence of the search warrant under 18 U.S.C. § 2705(b).

**CONCLUSION**

34. Based on my training and experience and the facts as set forth in this Affidavit, there is probable cause to believe that the unknown individual using the account rickpaul38@gmail.com violated 21 U.S.C. § 841 (Distribution of a Controlled Substance) and § 846 (Conspiracy to Distribute a Controlled Substance). There is also probable cause that evidence of these crimes will be found in the account of rickpaul38@gmail.com.



FRANK E. FEDEN  
Special Agent  
US Drug Enforcement Administration

SUBSCRIBED TO AND SWORN before me this 22 day of August, 2018.



SUSAN M. BAZIS  
United States Magistrate Judge  
District of Nebraska

**ATTACHMENT A**

**Property to be searched**

This warrant applies to information associated with [rickpaul38@gmail.com](mailto:rickpaul38@gmail.com) that is stored at premises owned, maintained, controlled, or operated by Google, Inc., a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.



## **ATTACHMENT B**

### **Items to be Seized**

#### **I. Information to be disclosed by Google Inc.**

This search warrant will be e-mailed or faxed to Google personnel by law enforcement agents. Google personnel are directed to isolate and disclose to the government the account and files described below related to the email accounts:

- rickpaul38@gmail.com for the period from the creation of the account to the date of this search warrant

1. All electronic mail stored and presently contained in, or on behalf of, the above email accounts, for the above specified periods.

2. All transactional information, session times and durations, content and connection log files of all activity for the above specified periods, by the users associated with the above referenced email account, including dates, times, methods of connecting (e.g., telnet, ftp, http), type of connection (e.g., modem, cable / DSL, T1 / LAN), ports used, telephone dial-up caller identification records, any other connection information or traffic data and records of the originating Internet Protocol Addresses of the user when he connected to Google.

3. All business records and subscriber information, in any form kept, pertaining to the above referenced email account, including applications, subscribers' full names, all screen names associated with the subscribers and/or email account, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, passwords, detailed billing records, types and lengths of service, and any other identifying information.

4. All instant messages stored and presently contained in, or on behalf of, the above referenced email account for the above specified periods.

5. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, location and direction information, files and data involved in the administration and management of websites, and other stored documents, notes, spread sheets and files.

6. All records and data related to mobile phones linked to, or accessing, the account, to include the unique identifiers such as IMEI numbers and contents of any mobile phone backups found within the account.

In order to minimize any disruption of computer service to innocent third parties, Google employees will create an exact duplicate of the computer accounts and files described above, including an exact duplicate of all information stored in the computer account and files described therein. Google employees will then provide the exact duplicate of the account and files described above and all information stored in those accounts and files to law enforcement agents, who need not be present during the duplication of the files, in electronic form not later than 7 days from the date of this search warrant.

## **II. Information to be seized by law enforcement as evidence**

Law enforcement personnel will thereafter review the information and files received from Google related to the email accounts:

- rickpaul38@gmail.com for the period from the creation of the account to the date of this search warrant

and then identify, copy and seize any evidence of violations of 21 U.S.C. §841 and 21 U.S.C. §846 including the following, all of which constitutes evidence:

1. Emails relating to the unauthorized importation, distribution, manufacture and sale of controlled substance or pharmaceutical drugs for the above specified period of time for the specified email account, including, without limitation, email communications (including email attachments) that are records of, or relate to:

a) the mailing, transportation, ordering, purchasing, receipt, manufacture, importation and/or distribution of controlled substance or pharmaceutical drugs:

b) financial transactions for the obtaining, secreting, transferring, importation and concealment of controlled substance or pharmaceutical drugs:

c) financial transactions evidencing expenditure of money made from engaging in illegal controlled substance or pharmaceutical drugs trafficking activity in, and/or importation of controlled substance or pharmaceutical drugs:

d) the ownership of assets obtained from illegal importation of, and/or trafficking controlled substance or pharmaceutical drugs:

e) Records of telephone numbers, address books, or papers which reflect names, addresses, and/or telephone numbers of associates and co-conspirators involved directly and indirectly in the smuggling and/or trafficking in controlled substance or pharmaceutical drugs and/or associates who have a monetary consideration and/or interest in the illegal smuggling or trafficking of controlled substance or pharmaceutical drugs: and

f) Correspondence that reflects the importation, trafficking, distribution, manufacture and/or mailing of counterfeit tobacco products:

2. All transactional information, session times and durations, content and connection log files of all activity for the above specified periods, by the users associated with the above referenced email accounts, including dates, times, methods of connecting (e.g., telnet, ftp, http), type of connection (e.g., modem, cable/DSL, T1/LAN), ports used, telephone dial-up caller identification records, any other connection information or traffic data and records of the originating Internet Protocol Addresses of the user when he connected to Google.

3. All business records and subscriber information, in any form kept, pertaining to the above referenced email accounts, including applications, subscribers' full names, all screen names associated with the subscribers and/or email accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, passwords, detailed billing records, types and lengths of service, and any other identifying information.

4. All instant messages stored and presently contained in, or on behalf of, the above referenced email accounts for the above specified period reflecting the importation, trafficking, distribution, manufacture and/or mailing of controlled substance or pharmaceutical drugs; and/or the handling of proceeds and assets obtained therefrom.

## UNITED STATES DISTRICT COURT

for the  
District of Nebraska

In the Matter of the Search of )  
(Briefly describe the property to be searched )  
or identify the person by name and address )

Information associated with rickpaul38@gmail.com that )  
is stored at premises controlled by Google Inc. )  
1600 Amphitheatre Parkway Mountain View, CA 94043 )

Case No. 8:18MJ324

**SEALED****SEARCH AND SEIZURE WARRANT**

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the \_\_\_\_\_ District of \_\_\_\_\_ Nebraska  
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

**YOU ARE COMMANDED** to execute this warrant on or before September 4, 2018 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.


The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Susan M. Bazis.

(United States Magistrate Judge)

☒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☒ for 30 days (not to exceed 30) ☐ until, the facts justifying, the later specific date of \_\_\_\_\_.

Date and time issued: 8-22-18 at 3:02 p.m.

  
\_\_\_\_\_  
Judge's signature

City and state: Omaha, Nebraska

Susan M. Bazis, United States Magistrate Judge

Printed name and title

**Return**Case No.:  
8:18MJ324

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Executing officer's signature*\_\_\_\_\_  
*Printed name and title*

**ATTACHMENT A**

**Property to be searched**

This warrant applies to information associated with [rickpaul38@gmail.com](mailto:rickpaul38@gmail.com) that is stored at premises owned, maintained, controlled, or operated by Google, Inc., a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

## **ATTACHMENT B**

### **Items to be Seized**

#### **I. Information to be disclosed by Google Inc.**

This search warrant will be e-mailed or faxed to Google personnel by law enforcement agents. Google personnel are directed to isolate and disclose to the government the account and files described below related to the email accounts:

- rickpaul38@gmail.com for the period from the creation of the account to the date of this search warrant

1. All electronic mail stored and presently contained in, or on behalf of, the above email accounts, for the above specified periods.

2. All transactional information, session times and durations, content and connection log files of all activity for the above specified periods, by the users associated with the above referenced email account, including dates, times, methods of connecting (e.g., telnet, ftp, http), type of connection (e.g., modem, cable / DSL, T1 / LAN), ports used, telephone dial-up caller identification records, any other connection information or traffic data and records of the originating Internet Protocol Addresses of the user when he connected to Google.

3. All business records and subscriber information, in any form kept, pertaining to the above referenced email account, including applications, subscribers' full names, all screen names associated with the subscribers and/or email account, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, passwords, detailed billing records, types and lengths of service, and any other identifying information.

4. All instant messages stored and presently contained in, or on behalf of, the above referenced email account for the above specified periods.

5. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, location and direction information, files and data involved in the administration and management of websites, and other stored documents, notes, spread sheets and files.

6. All records and data related to mobile phones linked to, or accessing, the account, to include the unique identifiers such as IMEI numbers and contents of any mobile phone backups found within the account.



In order to minimize any disruption of computer service to innocent third parties, Google employees will create an exact duplicate of the computer accounts and files described above, including an exact duplicate of all information stored in the computer account and files described therein. Google employees will then provide the exact duplicate of the account and files described above and all information stored in those accounts and files to law enforcement agents, who need not be present during the duplication of the files, in electronic form not later than 7 days from the date of this search warrant.

## **II. Information to be seized by law enforcement as evidence**

Law enforcement personnel will thereafter review the information and files received from Google related to the email accounts:

- rickpaul38@gmail.com for the period from the creation of the account to the date of this search warrant

and then identify, copy and seize any evidence of violations of 21 U.S.C. §841 and 21 U.S.C. §846 including the following, all of which constitutes evidence:

1. Emails relating to the unauthorized importation, distribution, manufacture and sale of controlled substance or pharmaceutical drugs for the above specified period of time for the specified email account, including, without limitation, email communications (including email attachments) that are records of, or relate to:

a) the mailing, transportation, ordering, purchasing, receipt, manufacture, importation and/or distribution of controlled substance or pharmaceutical drugs:

b) financial transactions for the obtaining, secreting, transferring, importation and concealment of controlled substance or pharmaceutical drugs:

c) financial transactions evidencing expenditure of money made from engaging in illegal controlled substance or pharmaceutical drugs trafficking activity in, and/or importation of controlled substance or pharmaceutical drugs:

d) the ownership of assets obtained from illegal importation of, and/or trafficking controlled substance or pharmaceutical drugs:

e) Records of telephone numbers, address books, or papers which reflect names, addresses, and/or telephone numbers of associates and co-conspirators involved directly and indirectly in the smuggling and/or trafficking in controlled substance or pharmaceutical drugs and/or associates who have a monetary consideration and/or interest in the illegal smuggling or trafficking of controlled substance or pharmaceutical drugs: and

f) Correspondence that reflects the importation, trafficking, distribution, manufacture and/or mailing of counterfeit tobacco products:

2. All transactional information, session times and durations, content and connection log files of all activity for the above specified periods, by the users associated with the above referenced email accounts, including dates, times, methods of connecting (e.g., telnet, ftp, http), type of connection (e.g., modem, cable/DSL, T1/LAN), ports used, telephone dial-up caller identification records, any other connection information or traffic data and records of the originating Internet Protocol Addresses of the user when he connected to Google.

3. All business records and subscriber information, in any form kept, pertaining to the above referenced email accounts, including applications, subscribers' full names, all screen names associated with the subscribers and/or email accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, passwords, detailed billing records, types and lengths of service, and any other identifying information.

4. All instant messages stored and presently contained in, or on behalf of, the above referenced email accounts for the above specified period reflecting the importation, trafficking, distribution, manufacture and/or mailing of controlled substance or pharmaceutical drugs; and/or the handling of proceeds and assets obtained therefrom.